IBM Global Technology Services
Thought Leadership White Paper

November 2012

The flexible workplace: Unlocking value in the “bring your own device” era

Contents

Executive summary

Sales of smartphones and media tablets like the Apple iPad are mounting, with analysts estimating there are over 1 billion smartphones currently in use.[1] Although consumer technology advances are nothing new, what has changed is the push to leverage smartphones and tablets to conduct business. As the consumerization of IT ushers in the "bring-your-own-device" (BYOD) era, employees expect a flexible workplace, with fast access to applications and information from virtually anywhere and on any device.

This new mindset of anytime, anywhere access brings significant impacts and consequences to the IT organization, which must try to balance the promise of greater productivity and worker satisfaction with the security concerns it creates. While some companies are issuing smartphones and tablets for employees, a growing majority of employees are bringing personally-owned devices to the workplace for business purposes—often without explicit company approval. This paper explores how organizations can derive business value in the BYOD era, while still providing a security-rich IT infrastructure and consistent service levels.

Behind the BYOD momentum

A recent Gartner report concluded that "the rise of 'bring your own device' programs is the single most radical shift in the economics of client computing for business since PCs invaded the workplace."[2] There are numerous reasons underlying the astonishing speed and depth at which this trend has taken root. For example:

- Many of these smartphones and tablets, along with the growing number of enterprise-class mobile applications, have powerful capabilities and applications. They now far exceed those of the "standard issue" device from the IT department, making them much more desirable.
- Consumer mobile devices have become so pervasive in daily life as a result of improvements in technology (for example, small size, instant on, wireless Internet connectivity and so on), and therefore there is a level of comfort does not exist with "corporate" devices. In fact, this probably reflects a cultural shift as much as a technological one.
- Companies are demanding their employees to do more with less. Today's employee is an increasingly empowered and technology-savvy knowledge worker. Employees are turning to whatever helps them achieve that goal—and in many cases, that is not the PC chained to an office desk.
- Many enterprises issue corporate-liable devices to a small subset of the company, such as sales. Although mobility requirements are increasing, most enterprises are not expanding their corporate-liable programs due to cost pressures. Instead, they are exploring the employee-liable model (BYOD) to deliver mobile services to a larger population of users at reduced cost.

Embracing BYOD across the organization

It may be tempting to ban the use of personally owned devices in the enterprise as a result of the added support and security complexities, but corporate policies that take a hard line may simply not be enforceable. Corporate smartphone and tablet users may circumvent corporate policy, putting the enterprise at greater risk. For instance, users may forward corporate email, documents and presentations to consumer services like Google Mail or Dropbox so they can be accessed from their smartphones and tablets, creating a kind of "shadow infrastructure" over which enterprises have little control and increases the risk of data leakage. In addition, not embracing BYOD can also lead to lower employee satisfaction and difficulty attracting and retaining top talent.

> *"IT managers and CIOs need to realize that even if they don't allow employees to use their own devices, they will find workarounds and BYOD will still seep into the enterprise. IT departments will need to find the right balance between giving employees the flexibility to use their own device for work and the potential security risks and costs of embracing BYOD." IDC, "Addressing security issues and concerns of Bring Your Own Device Initiatives," June 2012.*[3]

So how do you say "yes" to personal devices without having the mess of governance, security, integration and support issues? By taking a methodical approach, rather than a reactive one. The following are a few key questions to consider:

- Mobile device support—What mobile devices will you support? What work needs to be done and where? While supporting a large variety of mobile devices will likely increase end-user satisfaction, this support can also increase costs, complexity and deployment time. For example, developing, deploying and securing mobile applications for multiple platforms (e.g., Apple iOS, Google Android, RIM BlackBerry, Windows Phone, etc.)
- Corporate culture and corporate policy—Does your company have a policy for the use of personally owned devices? Is the policy voluntary? What corporate data can be accessed? What is the security policy? Will you have a re-imbursement policy for mobile expenses? (e.g. device, voice, data) What is the corporate culture for mobile workers and does it align with your organization's strategy? Do you need to separate work and personal data on mobile devices? Do you have a strategy in place to handle lost or stolen devices and employee separation?
- Information Technology—What IT solutions do you need to implement your strategy? How do you manage and secure mobile devices? What is your mobile application strategy? How will you support a wide range of mobile devices? How do you monitor compliance with corporate policy?

End-user support for BYOD

With a wide range of smartphones and platforms to support, the help desk can quickly become overwhelmed. Self-service support and automation can help address these concerns. Specific capabilities can include:

- Up-to-date online documentation with device, platforms, services provided and employee responsibilities
- The ability to activate a new device online without administrative interaction
- Heavy use of social media inside the company to leverage "wisdom of the crowds" This is critical as new devices and OS versions are released weekly
- The ability to perform common tasks online including device reset and wipe

Matching solutions to your strategy

Once you have carefully considered your BYOD strategy, you will want to explore IT solutions that can successfully carry it out. The following are a few key areas you may want to consider:

- **Security:** How will you manage and secure mobile devices and data? Do you need to segregate work and personal data? How do you remove corporate data if the employee leaves the company or changes job roles? How do you check the security posture of the device before it is allowed to connect to the corporate network? (e.g. is the device jailbroken or rooted?)
- **Applications:** What applications will users use? Are they available out of the box? Are they web, native, hybrid or virtual? Do they meet my security requirements? Do I need to create custom applications? Do you need to explore Mobile Enterprise Application Platforms? (MEAP). How will you deploy and manage application? Do you need an enterprise application store to manage and distribute applications? Should you prohibit the applications that users can access on their mobile devices? Are there required applications that must run on the device? Are there applications that cannot run on the device? How will you update applications?
- **Network:** How will users connect their devices to the corporate network via Wi-Fi and cellular? If employees are connecting to the corporate Wi-Fi network, is there adequate Wi-Fi coverage and capacity? If employees are connecting from offsite, do I need one or more VPN solutions? How will you manage the added complexity and network traffic these devices could bring?
- **Support:** How will you provide support for a variety of devices? Will you automate common tasks such as device registration to reduce administration overhead? How will you educate employees on how to use mobile devices effectively?

Journey to mobility: Lessons learned

More than half of IBM's global employee population is mobile. The company needed to expand its corporate mobility program—launched in 2004 with a single corporate-issued device—to accommodate a variety of new mobile platforms entering the workplace. In 2009, IBM undertook an aggressive campaign to support enterprise mobility and smartphones and tablets in particular.

Over the course of three years, IBM piloted mobile access with different devices and operating systems, adding new entries like tablets as the market produced them. IBM collaboration software became an integral part of the solution. By 2011, wide-scale production deployment was under way, with mobility viewed as a core infrastructure service and in excess of 100,000 smartphone and tablet users with access to the IBM corporate network. Today, the program covers 120,000 mobile users, including 80,000 personally owned devices, and continues to expand.

The following are a few of the key lessons learned:

- Employees are supportive of personally owned (and funded) smartphones and tablets
- Employees want to use a single smartphone for personal and business use. Most users don't want to use two smartphones—one for work and one for personal use
- The majority of employees were supportive of the devices and platforms that IBM elected to support (e.g. Android 2.2+, iPhone 3GS+, BlackBerry, etc.). However, there were additional devices and platforms that employees asked for that could not be supported due to security requirements
- Generally, employees appreciated the need to enforce security policies on the device. However, this was a deal-breaker for some users. The biggest customer dissatisfier is the eight-character alphanumeric password to unlock the device. Employees want better authentication techniques and the ability to be prompted for a password when accessing "work" data.
- For security purposes, there needs to be better containerization solutions to separate work and personal data and the ability to manage all work data as a single container. This reduces the need to secure each application individually.
- Remote wipe of an entire device is unpopular with employees. Employees applauded the enhancements to Lotus Traveler which allows remote wipe of just corporate data (e.g. email)
- Browser-based cloud solutions like IBM® Lotus® iNotes® ultra-light mode provides flexibility, reduces device dependencies and addresses data at rest security concerns
- With multiple smartphone and tablet options, we needed to provide guidance to employees so they could make informed choices on what the best device(s) were for their particular needs
- Leveraging Lotus Mobile Connect clientless SSL proxy provided the best end-user experience on Apple iOS and Google Android. However, this necessitated the use of a separate, VPN client solution for general access to the corporate network.
- Employees were receptive of self-service support options including automated onboarding and diagnostics

IBM Mobile chronology

2004 - 2007: BlackBerry smartphone is the sole option, with limited employee access

2008: Limited proof of concept for Windows Mobile leveraging IBM Lotus Traveler

2009: Launched pilot and expanded to include Nokia and Apple iOS and embraced personally owned model with expanded access via Lotus Traveler

2010: Completed pilot and began production deployment. Expanded platform support to include Apple iPad and Google Android

2011: Offered wide-scale production deployments to support increased usage of mobile as primary computing device (replacing laptops), with native mobile clients for Sametime Instant Messaging, IBM Connections and Symphony Viewers on Apple iOS and Android in addition to custom mobile application developed in house and deployed via an internal application store.

2012: Launched IBM Mobile Enterprise initiative. Cross IBM software, hardware and services launched to help clients transform their enterprises with Mobile solutions for "front-office" and "back-office" applications.

Conclusion

Far from declining, the BYOD momentum continues to expand as more employees demand a flexible workplace that allows them to access the tools they need anywhere and from any device. Forward-thinking organizations are looking for ways to successfully implement a flexible mobile environment that supports employee choice, enables secure access to enterprise data and applications, and allows personally owned devices to co-exist in the infrastructure with corporate-issued and special-purpose wireless devices. Such a transformation is already happening inside IBM.

In addition to our own well-documented transformation into a mobile enterprise, IBM has been providing mobility solutions for hundreds of clients for more than 15 years, IBM professionals have developed robust solutions to support global security, support and applications needs, enabling our services to expand across additional leading mobile platforms and devices. Backed by a rich business-partner ecosystem, IBM can help you understand mobile requirements, begin to assess your current environment and design a strategy for mobile device management.

For more information

To learn more about IBM Enterprise Services—managed mobility services, contact your IBM marketing representative, IBM Business Partner, or visit the following website: **ibm.com**/services/mobility

IBM Global Services
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
November 2012

[1] Strategy Analytics, “Global Smartphone Installed Base Forecast by Operating System for 88 Countries: 2007 to 2017.” October 2012.

[2] Gartner, “Bring Your Own Device: New Opportunities, New Challenges,” August 2012. Doc # G00238131

[3] IDC, “Addressing Security Issues and Concerns of Bring - Your -Own - Device Initiatives.” June 2012. Doc # AE53U